EXHIBIT 10

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

In re *Inter Partes* Review of:
U.S. Patent No. 7,835,689

For: DISTRIBUTION OF MUSIC BETWEEN MEMBERS OF A CLUSTER OF MOBILE AUDIO DEVICES AND A WIDE AREA NETWORK

DECLARATION OF KEVIN C. ALMEROTH, PH.D.

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
US Patent and Trademark Office
PO Box 1450
Alexandria, Virginia 22313-1450

I, Kevin C. Almeroth, hereby declare and state as follows:

1. I have been retained as a technical consultant on behalf of Samsung Electronics Co., Ltd., the petitioner in the present proceeding, and I am being compensated at my usual and customary hourly rate. The petition names Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., and Samsung Telecommunications America, LLC as real parties-in-interest. I have no financial interest in, or affiliation with, the petitioner, real parties-in-interest, or the patent owner, which I understand to be BLACK HILLS

MEDIA, LLC. My compensation is not dependent upon the outcome of, or my testimony in, the present *inter partes* review or any litigation proceedings.

2. I have reviewed each of the following:

a. U.S. Patent No. 7,835,689 ("the '689 Patent"), including the claims, description and prosecution history (which is identified in the Petition respectively as Exhibits 1001 and 1002);

b. U.S. Patent No. 7,383,433 to Yeager et al. (which is identified in the Petition as Exhibit 1003; hereinafter "Yeager");

c. Manoj Parameswaran *et al.*, *P2P Networking: An Information-Sharing Alternative*, Computer 31-38 (July 2001) (which is identified in the Petition as Exhibit 1005; hereinafter "*P2P Networking*");

d. U.S. Patent App. Pub. No. 2002/0087887 to Busam *et al.* (which is identified in the Petition as Exhibit 1006; hereinafter "Busam");

e. U.S. Patent No. 7,058,696 to Phillips *et al.* (which is identified in the Petition as Exhibit 1007; hereinafter "Phillips");

f. U.S. Patent No. 6,192,340 to Abecassis (which is identified in the Petition as Exhibit 1008; hereinafter "Abecassis"); and

g. U.S. Patent No. 5,535,276 to Ganesan (which is identified in the Petition as Exhibit 1009; hereinafter "Ganesan").

3. Upon reviewing the ’689 Patent, I understand that a non-provisional application was filed on December 4, 2006 (Appl. No. 11/566,552), which issued as the ’689 Patent. I further understand that the ’689 Patent claims priority to a provisional application (Appl. No. 60/378,415) filed on May 6, 2002. For the purposes of my analysis, I assume the time of the purported invention to be no earlier than May 2002.

4. It is my opinion that a person of ordinary skill in the art at the time of the inventions claimed in the ’689 Patent would have typically had a M.S. degree in computer science in addition to two or more years of work experience relating to the distribution of multimedia content over networks. I was a person of skill in this art in May 2002.

5. My background, qualifications, and experience relevant to the issues in proceeding are summarized below. My *curriculum vitae* is submitted herewith as Exhibit 1012.

6. I am currently a Professor in the Department of Computer Science at the University of California, Santa Barbara. At UCSB, I also hold faculty appointments and am a founding member of the Computer Engineering (CE) Program, Media Arts and Technology (MAT) Program, and the Technology Management Program (TMP). I have been a faculty member at UCSB since July 1997.

7. I hold three degrees from the Georgia Institute of Technology: (1) a Bachelor of Science degree in Information and Computer Science (with minors in Economics, Technical Communication, and American Literature) earned in June, 1992; (2) a Master of Science degree in Computer Science (with specialization in Networking and Systems) earned in June, 1994; and (3) a Doctor of Philosophy (Ph.D.) degree in Computer Science (Dissertation Title: Networking and System Support for the Efficient, Scalable Delivery of Services in Interactive Multimedia System, minor in Telecommunications Public Policy) earned in June, 1997.

8. One of the major concentrations of my research to date has been the delivery of multimedia content and data between computing devices. In my research, I have studied large-scale content delivery systems, and the use of servers located in a variety of geographic locations to provide scalable delivery to hundreds, even thousands of users simultaneously. I have also studied smaller-scale content delivery systems in which content is exchanged between individual computers and portable devices. My work has emphasized the exchange of content more efficiently across computer networks, including the scalable delivery of content to many users, mobile computing, satellite networking, delivering content to mobile devices, and network support for data delivery in wireless networks.

9. In 1992, at the time I started graduate school, my research focused initially on interactive functions (*e.g.*, VCR-style functions like pause, rewind, and fast-forward) for near video-on-demand systems in cable systems. This included handling multiple requests using one audio/video stream broadcast to multiple receivers simultaneously. This research has developed into new techniques to deliver on-demand content, including audio, video, web documents, and other types of data, through the Internet and over other types of networks, in a way that scales to a large number of users.

10. In 1994, I began to research issues associated with the development and deployment of multicast in the Internet. Multicast allows scalable transmission from a single source to an arbitrary number of receivers. Some of my more recent research endeavors have looked at how to use the scalability offered by multicast to provide streaming media support for complex applications like distance learning, distributed collaboration, distributed games, and large-scale wireless communication.

11. Starting in 1997, I worked on a project called the Interactive Multimedia Jukebox ("IMJ") to integrate the streaming media capabilities of the Internet together with the interactivity of the web. Users could select content to view from a website, which would then be scheduled for delivery using multicast on one of a number of logical content streams. Delivery would be scheduled

according to available communication capacity: if idle capacity existed when a request was made, the requesting user would be able to watch its selection immediately. If the server was fully utilized in streaming previously selected content, the user's selection would be queued. In the meantime, the user would see what content was already playing, and because of the use of multicast, would be able to join one of the existing streams and watch the content at the point it was currently being transmitted. This service combined the interactivity of the web with the streaming capabilities of the Internet to create a jukebox-like service. As part of the project, we obtained permission from Turner Broadcasting to transmit cartoons and other short-subject content.

12. In the course of my research, I have been involved in the development of academic research into available technology in the marketplace. One aspect of this work is my involvement in the Internet Engineering Task Force (IETF), including many content delivery-related working groups like the Audio Video Transport (AVT) group, the MBone Deployment (MBONED) group, the Source Specific Multicast (SSM) group, the Inter-Domain Multicast Routing (IDMR) group, the Reliable Multicast Transport (RMT) group, the Protocol Independent Multicast (PIM) group, etc. I have also served as a member of the Multicast Directorate (MADDOGS), which

oversaw the standardization of all things related to multicast in the IETF. Finally, I was the Chair of the Internet2 Multicast Working Group for seven years.

13. I am an author or co-author of nearly 200 technical papers, published software systems, IETF Internet Drafts, and IETF Request for Comments (RFCs). The titles and subject matter of these technical papers are listed in full on my CV, which is identified in the petition as Exhibit 1012. Furthermore, in the courses I teach at UCSB, a significant portion of my curriculum covers aspects of the Internet and network communication including the physical and data link layers of the Open System Interconnect (OSI) protocol stack, and standardized protocols for communicating across a variety of physical media such as cable systems, telephone lines, wireless, and high-speed Local Area Networks (LANs). The courses I have taught also cover most major topics in Internet communication, including data communication, multimedia encoding, and (mobile) application design. For a complete list of courses I have taught, see my *curriculum vitae*, Exhibit 1012.

State of the Art Through 2001

14. One of the most widely deployed computer networks, *i.e.*, physical connections of computers to exchange data, is the Internet. The Internet has been around for several decades, with many tracing its origins to the ARPAnet

in the late 1960s. While the origins of the Internet were humble, it has grown into a massive, highly sophisticated network for highly complex and highly varied forms of communication. Originally useful mainly for the exchange of text documents through email or file exchange, the Internet has evolved to support more complex data transactions including multiple media types (*e.g.*, audio, video), hence the concept of "multimedia." Coupled with new and improved delivery capabilities and increased ways of offering information to users, the ways in which the Internet could be used increased dramatically during the 1990s. These factors led to numerous technical innovations in the way data was made available to users.

15. By 2001, these users had multiple options for playing media available on the Internet. Many software programs, such as RealAudio Player and CU-SeeMe, were available that allowed general purpose computers (both desktop and laptop computers) to play multimedia files and stream either audio or video content. Ex. 1013, Savetz *et al.*, *MBONE: Multicasting Tomorrow's Internet*, pp. 25-31 (1996) (hereinafter "Savetz"). Portable media players, including hand-held mp3 players like the Diamond Rio PMP300, Creative Nomad Digital Audio Player, and iPod®, were also available by 2001.

16. By 1993, a popular early internet videoconferencing application called CU-SeeMe was released. Ex. 1013, Savetz, p. 27. CU-SeeMe allowed users to

engage in two-way videoconferencing with real-time interactive video and voice communications over the Internet. *Id.* at 25. CU-SeeMe also used a server-like component called a "reflector," that would enable group videoconferencing, in which some users would only receive communications, as seen below:

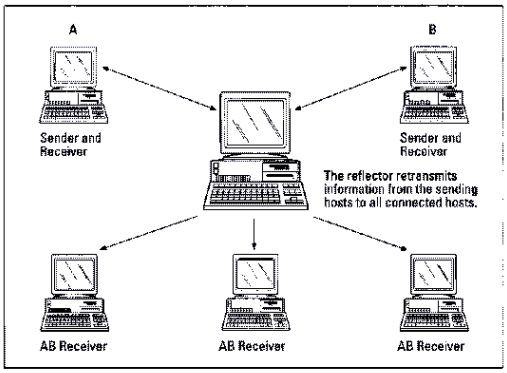

Figure 2-5: How a reflector works.

. *Id.* at 25-26.

17. But CU-SeeMe's applications went far beyond simple "talking-heads style videoconferencing." Ex. 1013, Savetz, p. 27. By 1996, CU-SeeMe had been used to broadcast speeches, lectures, and the Internet's first full-length movie (an indie comedy called *Party Girl* starring Parker Posey). *Id.*

18. Given bandwidth constraints prevalent in the early- to mid- 1990s, CU-SeeMe's reflector did not scale well for large groups because it would need to send a separate stream of unicast IP packets to each user who wanted to receive the signal. Ex. 1013, Savetz, pp. 25-26. Thus, a five-person videoconference would require five times the bandwidth of a single signal.

Id. at 26. These bandwidth constraints led others to implement videoconferencing technology using a more efficient multicasting protocol. *Id.* at 60.

19. Multicasting involves transmission to many users (often from a single source). Ex. 1014, Kevin C. Almeroth, *The Evolution of Multicast: From the MBone to Interdomain Multicast to Internet2 Deployment*, IEEE Network 10-20 (Jan./Feb. 2000) at 10 (hereinafter "Almeroth"). Thus, multicasting can be used for a variety of applications ranging from broadcasting large sports events to small group videoconferences. But rather than use a broadcast medium, multicasting uses a network like the Internet.

20. By 1995, it was well known that media content could be efficiently distributed over a network through the use of multicast trees. Ex. 1015, Li Gong & Nachum Shacham, *Multicast Security and Its Extension to a Mobile Environment*, 1 Wireless Networks 281-295 (1995) at 282 (hereinafter "*Multicast Security*"). A multicast tree begins with traffic from a content source that is injected at the root node of the tree. *Id.* The root sends this traffic to its child nodes. *Id.* These nodes then replicate that traffic to their children. *Id.* Each subsequent node receives traffic from its parent node and replicates that traffic to its child nodes. *Id.*

21. By 1992, a system known as the Multicast Backbone ("MBone" or "M-Bone") had been used to broadcast a live audiostream of an Internet Engineering Task Force meeting to over 20 participants. Ex. 1014, Almeroth, p. 11. By 1994, the Rolling Stones had used M-Bone to broadcast a live concert over the Internet. Ex. 1016, Neil Strauss, *Rolling Stones Live on Internet*, The New York Times, Nov. 22, 1994. No later than 1996, M-Bone had been used for video teleconferences. Ex. 1013, Savetz, p. 60.

22. Another popular method for media sharing amongst internet users involved peer-to-peer networks. Ex. 1017, Karl T. Greenfeld, *Meet the Napster*, TIME 60-68 (October 2, 2000) (hereinafter "Greenfeld"). The networks were frequently used as file sharing programs that allowed computer users to share media files, such as mp3s, across both local and wide-area networks. *Id.* at 64. The most famous of these programs, Napster, was released in 1999. *Id.* at 62. By 2000, Napster had over 25 million users and was featured on the cover of Time Magazine. *Id.* at 62, cover. Napster allowed users to locate songs in mp3 format on other users' computers by searching a central server that contained information about these songs. *Id.* at 62. After locating each other through the central server, Napster users could share songs on a peer-to-peer basis (*i.e.*, directly from one user's computer to another user's computer). *Id.* at 62.

23. Other fully decentralized peer-to-peer file sharing systems like Gnutella, which was released in 2000, allowed users to search for media on other users' computers without a central server. Ex. 1018, Gene Kan, *Gnutella*, pp. 97-100, *in* Peer-to-Peer: Harnessing the Power of Disruptive Technologies (Andy Oram ed., 2001) (hereinafter "Kan").

24. By 2001, both peer-to-peer file sharing users and multicast videoconferencing users had demonstrated a need for secure private group sharing. Decentralized peer-to-peer file sharing networks like Gnutella could be disrupted if either malicious users or too many users joined a network. Ex. 1018, Kan, pp. 114-115. There was also a need to provide secure file sharing amongst political activists in repressive countries. Ex. 1019, John Schwartz, *File-Swapping Is New Route for Pornography on Internet*, The New York Times, July 28, 2001. And there was a well-known desire to use multicast videoconferencing for highly confidential applications, such as a meeting between geographically dispersed corporate executives. Ex. 1015, *Multicast Security*, p. 293. By 2001, both peer-to-peer file sharing systems and multicast videoconferencing systems had been created to meet these needs for secure private group sharing.

25. For example, by 2001, multicast videoconferencing technology allowed users to create private sessions both through controlling the multicast tree and

through encryption. Ex. 1015, *Multicast Security*, pp. 282-285. As described above, multicast trees begin with a root source, where traffic is injected into the tree. *Id.* at 282. By 1995, a multicast protocol existed that would allow new recipients to join the multicast tree only with approval from the source. *Id.* Encrypted multicast protocols also existed that would provide for secure multicast groups. *Id.* at 283-285. Admission to a secure group could require either all existing members of the group to approve the new member or an elected, trusted group leader to approve the new member. *Id.* at 283-284.

26. Also by 2001, Gnutella clients allowed users to create private sharing groups that could be joined only by users that knew the group's secret handshake or password. Ex. 1018, Kan, p. 115. These private Gnutella groups ensured a high quality of service by controlling the size of the network and the type of users on the network. *Id.*

27. Finally, by 2001, instant messaging software, such as Aimster and Windows Messaging, allowed users to share media files only with their designated messaging "buddies." Ex. 1020, David Kushner, *The Digital Beat: The Instant Message Music War*, Rolling Stone, June 13, 2001 (hereinafter "Kushner"). These messages would be encrypted to ensure secure transmission. Ex. 1019, Schwartz.

Overview of the '689 Patent

28. The '689 Patent addresses a method and device for sharing media amongst a group of users, wherein a user's ability to join a sharing group is based on information about that user that is made available by a trusted user. The patent discloses numerous embodiments for accomplishing this media sharing, including embodiments of mobile devices for sharing audio entertainment, *see, e.g.*, '689 Patent, 3:31-48, 5:19-31, and embodiments of audio entertainment devices for sharing that need not be mobile, *see, e.g.*, '689 Patent, 3:15-30, 3:49-58, 4:4-22, 4:23-40. And the patent contemplates sharing audio, video, or a combination of both. '689 Patent, 56:17-19.

29. For example, the '689 Patent discloses that decisions on admitting a requesting user to such a sharing group may be made based on rating information regarding the requesting member, the duration of the requesting member's association with other sharing groups, and the popularity of such other sharing groups. '689 Patent, 37:64 – 38:10. Moreover, the '689 Patent discloses that the decision of whether to admit the requesting user to the sharing group may be based on information on the reputation or desirability of the requesting user as retrieved from trusted people.

Claim Construction

30. I have been asked to offer my opinion regarding the understanding of a person skilled in the art regarding certain claim terms in the '689 Patent. I understand that in the present proceeding, claim terms are interpreted as the broadest reasonable construction consistent with the specification or "BRC."

31. I have been asked to offer my opinion about the understanding of a person skilled in the art regarding the term "media player device," which appears in each of independent claims 1 and 11. As discussed above in Paragraph 15, a person of ordinary skill in the art would have understood that general purpose computers (both desktops and laptops) could play media when loaded with appropriate software. Further, a person of ordinary skill in the art would have been familiar with hand held portable media players, like the iPod®. The '689 Patent anticipates using both types of media players because it discloses both mobile device embodiments for sharing audio entertainment, *see, e.g.*, '689 Patent, 3:31-48, 5:19-31, and other embodiments for sharing audio entertainment that need not be mobile, *see, e.g.*, '689 Patent, 3:15-30, 3:49-58, 4:4-22, 4:23-40. Because the state of the art and the '689 Patent recognize both mobile and non-mobile media players, the scope of the term "media player device" should not be limited to mobile embodiments.

32. One of skill in the art would also understand that the ’689 Patent discloses media players that may “comprise video or audio/visual players.” ’689 Patent, 56:17-38. Based on such disclosures, in my opinion, one skilled in the art would understand that a “media player device” to be “a device that is capable of playing media, including audio content, video content, or a combination of both.”

33. I have also been asked to offer my opinion about the understanding of a person skilled in the art regarding the term “information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group,” which is recited in independent claim 9. In my opinion, a person skilled in the art would understand that the broadest reasonable construction for this “information” must include within its scope any information, such as a password, security certificate, or other form of credential, provided by a “trusted user” to the “user of the requesting media player device” that can be used to access a sharing group. For example, when a trusted user extends an invitation and provides a password that allows a user to join the sharing group, one skilled in the art would understand that password as representing “information, made available by a trusted user, regarding the desirability of the [requesting] user” because it would be more

difficult for the requesting user to join the sharing group without the password.

The Yeager Patent

34. Yeager discloses several improvements to prior art peer-to-peer networks, such as Napster and Gnutella, that were famously used to share media content. *See, e.g.*, Yeager, 2:17-23. A person skilled in the art at the time would understand that any discussion of peer-to-peer networking technology would be read in light of the explosive success that media sharing networks like Napster had, and thus would be motivated to combine any new peer-to-peer technology with media sharing.

35. Further, Yeager discloses that a variety of portable devices, including phones and PDAs, can be peers, *see, e.g.*, Yeager, 7:30-35, 8:13-22, 27:51-62. A person skilled in the art at the time would understand that such portable devices were capable of being media player devices because portable media players were well known by that time, s*ee supra* ¶ 15, and because peer nodes were frequently used to access and play media content from peer-to-peer networks such as Napster and Gnutella.

36. The first improvement that Yeager discloses that peer groups can be formed on these peer-to-peer networks to share protected content. Yeager, 28:1-6,

37:9-20, 37:35-50. Although "new peers . . . may not initially belong to any peer group," Yeager, 7:20-21, peers can request to join existing peer groups. Yeager, 35:59-61, 52:15-51.

37. Second, Yeager discloses methods for determining whether to trust another user based on content quality and risk. *See, e.g.*, Yeager, 7:6-8. Yeager recognized that prior art methods for assessing trust were "too biased toward personal risk and not content," and that "it may [be] desirable that trust be biased towards data relevance." Yeager, 1:47-50. A person skilled in the art would understand this disclosure to teach rating both peers and content shared by peers under a variety of metrics that assess both risk (*e.g.*, of a slow connection or of malicious behavior) and the quality of content (*e.g.*, quality of music files or recipes being shared).

38. Finally, Yeager discloses multiple ways to allow trusted users to provide input on whether a user's request to join a peer group should be granted. In the first method, one or more trusted users will directly make a decision about whether the requesting user should be allowed to join the group based on information about the requesting user. Yeager, 35:59-36:3, 57:25-29. A person skilled in the art would understand that the "representative member peer" that is elected to "accept or reject new membership applications" is trusted by the other group members to make important decisions about which peers should be

allowed to access the protected content being shared by the group. Yeager, 35:59-36:3, 37:9-20. A person skilled in the art would also understand that the trusted user's decision would be based on, among other things, a determination about whether the peer passes a cooperation threshold based on an assessment of the peer's content quality and personal risk. Yeager, 10:14-18; 11:23-26; 27:63-28:8; 40:4-9.

39. Another method disclosed by Yeager involves allowing trusted users to sign security certificates that the requesting user submits to authenticate her identity during a join request. Yeager, 17:12-33, 18:40-65, 52:23-51.

The *P2P Networking* Reference

40. The *P2P Networking* reference discloses why it is desirable to set up peer-to-peer networks with controlled memberships. *P2P Networking* discloses that the extreme flexibility of open peer-to-peer networks is disadvantageous because it leads to a great variance in content quality and connections speeds. *P2P Networking*, p. 34. Open peer-to-peer networks also suffer from malicious users that can distribute undesirable content. *Id.* at 35.

41. *P2P Networking* also discloses a solution to the problems of open networks: private peer-to-peer networks with controlled memberships that can classify content and exclude undesirable users using feedback scores "similar to the

scores that eBay provides for auctioneers." *P2P Networking*, p. 34. Further, *P2P Networking* discloses that by restricting participation to exclude free riders, a private network would discourage copyright infringement prevalent on other peer-to-peer networks. *Id.* at 35.

The Combination of Yeager and *P2P Networking*

42. The Yeager patent discloses all the limitations of Claims 9 and 10 of the '689 Patent. It discloses "sharing groups" in the form of "peer groups" that are used to publish content. Yeager, 28:1-6, 37:9-20, 37:35-50. And it discloses that existing members of a peer group will receive requests to join the peer group from potential new members. Yeager, 35:59-61, 52:26-41. Yeager further discloses making a determination about whether to admit that requesting peer based two types of information associated with the user of that peer: credentials that may be signed by a trusted user (Yeager, 17:12-33, 18:40-65, 52:23-51.); and trust levels that a trusted user will review to determine whether the join request should be granted (Yeager, 10:14-18, 11:23-26, 27:63-28:8, 35:59-36:3, 40:4-9, 57:25-29). Finally, Yeager discloses adding the requesting peer to the sharing group by distributing a full membership credential to the requesting device. Yeager, 52:52-63.

43. *P2P Networking* discloses why the limitations in Yeager would be combined in the way that they are in Claims 9 and 10 of the '689 Patent. *P2P*

Networking discloses that it is desirable to create a "self-enforced, restricted membership social community like a neighborhood P2P network" so that "users can impose standards on the quality of content and service." *P2P Networking*, p. 36. *P2P Networking* further discloses that such a network can be established through rating users based on content contributions and connection speeds in order to exclude free riders, malicious users, and low-speed nodes. *Id.* at 34-35.

44. A person skilled in the art would have had reason to combine the elements disclosed in Yeager to achieve the purpose disclosed in *P2P Networking* because both references arise from the same narrow field of art: content sharing on peer-to-peer networks. Moreover, both references disclose allowing users to rate peers and content quality in order create curated communities, like private peer-to-peer networks and peer groups focused on a particular interest. *See* Yeager, 6:56-7:10; *P2P Networking*, pp. 34-36.

The Busam Application

45. Busam discloses a device-to-device network in which users are organized in sharing groups so that their devices can share and stream media files to and from each other. Busam, [0008], [0028], [0032], Fig. 1. Busam further discloses an embodiment in which new devices must send requests to obtain

access to shared devices on device-to-device networks. Busam, [0008]-[0009], [0025], [0028].

46. The sharing device described in Busam "can be a computer, a browser running on a computer, a digital music player running on a computer, a stand-alone music player, a video player, etc." Busam, [0025]. And these devices can share music by either transferring or streaming music files. Busam, [0008].

47. Busam further discloses an embodiment in which two devices, Device A and Device B, set up a device-to-device network and authenticate with each other by exchanging usernames and passwords associated with each device. Busam, [0048], Fig. 12. If those usernames and passwords are from the same sharing group, those devices will be able to share media content with each other. Busam, [0028], [0048]. Busam further discloses that those devices receive a broadcast request from a third device, Device C, to join their device-to-device network and to be authenticated as part of the same user group. Busam, [0048], Fig. 12. After Device C authenticates with both devices by sharing a username and password, "all three devices are on the device-to-device network and can access each other." Busam, [0048].

The Phillips Patent

48. Phillips discloses a multi-user shared file access service in which users belong to user groups that can access shared files. Phillips, 1:40-42, 5:66-6:9. The users can operate client nodes—such as computers, game consoles or internet receivers—and access file groups. Phillips, 6:1-9, 8:43-46. The shared files are stored in virtual storage devices on a remote file server node, with each virtual storage device being accessible by a different group of users. Phillips, 9:60 - 10:9.

49. These virtual storage devices are managed by a client manager node that is "able to designate new user accounts and to provide sufficient information to enable a client user to join one or more of the virtual storage devices." Phillips, 12:36-39. The user of the client manager node can invite new users to join by sending them emailed invitations containing "one time passwords" (OTP). Phillips, 16:22-28, 16:50-60. "The purpose of the client manager node is to provide the customer" with the ability to designate a trusted user that—in addition to designating new user accounts—can also "administer each of the [customer's] virtual storage devices," and "is provided with full access privileges for all of the files and directories on each virtual storage device." Phillips, 12:21-39. In my opinion, a person of ordinary skill in the

art would understand that these significant administrative rights and privileges would be given only to trusted users of a sharing system.

50. A person skilled in the art would understand that the client manager node would be able to employ a variety of metrics to determine which users should receive invitations. Given the overall focus on security in Phillips, a person skilled in the art at the time would understand that the client manager node would not want to send an invitation to an untrustworthy or otherwise undesirable user.

51. New client users can then request to join a user group by clicking on an emailed invitation "at a particular client node." Phillips, 17:9-11, 18:16-18, Fig. 6B. A determination is then made as to whether the new client user's node will be allowed to join the user group based on the user's user ID and OTP. Phillips, 16:50-51, 17:9-11, 18:16-18, 18:22-36, Fig. 6B.

The Combination of Busam and Phillips

52. The Busam application discloses a device-to-device network for sharing and streaming media. Devices on this network can be any kind of media player device, ranging from a web browser to a portable music player to a car stereo. Busam, [0025], [0027]. These devices are associated with users, who are organized into sharing groups. Busam, [0028]. Devices can only see (and

hence share media with) other devices in their sharing group. Busam, [0028]; [0034].

53. The Phillips patent discloses a file sharing system in which groups of users receive access to virtual storage devices. Users will access the virtual storage devices through client nodes, which can be a variety of computers, including game consoles and internet receivers. Phillips, 8:43-46. New users can request to join an existing user group, but they will only be allowed to join if the user of the client manager node has sent them a one-time password to indicate that they are allowed to join the group. Phillips, 16:50-51, 17:9-11, 18:16-18, 18:22-36, Fig. 6B.

54. In my opinion, a person of ordinary skill in the art would have had reason to combine the teachings of the Busam application with the teachings of the Phillips patent because both references teach ways for devices to share content amongst users in a group. By the critical date, it had become desirable to do more than just share files for the purpose of exchanging and archiving. There was a well-known desire to distribute content amongst different Internet users for collaborating on projects and consuming media. A person of ordinary skill in the art would have reason to use Phillips' method of file sharing to share media content, as is disclosed in Busam, because it was well known at the time that file sharing systems could be used to share media (*e.g.*, Napster).

55. Further, a person of ordinary skill in the art would have had reason to combine Phillips' method for verifying new users with a one-time password from a trusted user with Busam's media sharing group because it was well known at the time that private media sharing groups could be protected by allowing a trusted user to share a password. *See supra* ¶ 26. The Phillips method offers an improvement to the method of choosing a single group password, by allowing each password to be used only one time. Phillips, 19:4-9. This improvement prevents existing users from usurping the trusted user's role of inviting new members by re-sharing the group password. Because this improvement was simply one of several known ways of limiting which users would be able to become members of a service. a person skilled in the art would be motivated by Busam's focus on limiting access to content, Busam, [0006], to screen new members with the more secure Phillips process.

56. Moreover, the combination of the Phillips patent and the Busam application provides the teaching that applicants argued was missing from the prior art regarding the "wherein" clause present in claim 9 - "wherein the information associated with the user of the requesting media player device comprises information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group." In particular, the Phillips patent discloses that a requesting user can join an

existing user group if the user is able to provide a one-time password that it received from a trusted user. Phillips, 16:50-51, 17:9-11, 18:16-18, 18:22-36, Fig. 6B.

The Abecassis Patent

57. Abecassis relates to a system and methods for providing content, such as music, to multimedia players. Abecassis, Abstract, 3:44-64. Abecassis discloses that the content can be obtained from central information providers, such as specialized servers, or multimedia players can exchange information between themselves directly. Abecassis, 13:62-14:7. Abecassis also discloses a network of digital audio devices that can retrieve and transmit audio and information from each other. Abecassis, 7:16-22, 11:1-30 and Fig. 4.

58. A person skilled in the art would understand that the network of devices disclosed in Abecassis is a "sharing group" because the devices on that network can share media content to and from each other.

59. The reference discloses that the user of an audio device may enter login/password information into his/her audio device to access services from the network. Abecassis, 19:38-20:16. The Abecassis patent discloses that if login is successful, processing continues, ultimately allowing the audio device to obtain services from an information-providing device (*i.e.*, receive and

transmit audio and information from other audio devices of the network). Abecassis, 11:1-8, 20:11-15, 27:11-18, Figs. 7 and 9.

60. It is my opinion that one of skill in the art would understand that this access control functionality could be located either in the media player device that is accessing shared content or another device on the network. The Abecassis patent indicates that such access control functionality is not necessarily located in the audio device of the user, and one skilled in the art would therefore understand that the access control could also reside in other audio devices already accessing the network. Abecassis, 27:1-4. Further, the Abecassis patent discloses access control in connection with "handshaking," indicating to one skilled in the art that the access control routines may be based in an audio device of the network other than the audio device attempting access to the network (*e.g.*, an information provider). Abecassis, 19:53-55 and 26:57 – 27:10.

The Ganesan Patent

61. The Ganesan patent discloses systems for maintaining the privacy of information transmitted across a communications channel. Ganesan, 1:9-19. In one system, a transmitter sends a message that is encrypted to a receiver along with a certificate that authenticates the identity of the transmitter to the receiver. Ganesan, 2:41-54. The authenticating certificate is generated by a

trusted third party, such as a Certificate Authority (CA) that serves as a trusted intermediary. Ganesan, 2:48-54 and 1:58-2:20. Moreover, the trusted third party, could, for example, be another user, such as an authentication server. Ganesan, Abstract, claims 1, 2 and 4, 8:20-43.

62. One skilled in the art would understand that the authenticating certificate corresponds to the "information associated with a user" that is "made available by a trusted user" as recited in claim 9 of the '689 Patent because the authenticating certificate relies on a trusted intermediary to identify the sender of a message.

The Combination of Abecassis and Ganesan

63. The Abecassis patent discloses an access control system that determines whether a user of a multimedia player device may obtain access to a sharing group (*i.e.*, network of devices) in which devices are sharing multimedia content. For example, in one embodiment, handshaking routines may request user identification, and, if required, a corresponding password. Abecassis, 19:49-59.

64. The Ganesan patent discloses that a first user, to assure a second user of the first user's identity, may send the second user a certificate issued by a trusted intermediary that attests to the identity of the first user. Ganesan, 2:48-54.

The Ganesan patent further indicates that the trusted intermediary may, for example, be another user of the system, such as an authentication server. Ganesan, 8:29-39.

65. A person skilled in the art would understand that successful authentication of a user by a content distribution system based on a third-party's statement, such as by a Certificate Authority, indicates that the user is authorized to access content on the content distribution system. This distinguishes a certified user from a user that is not successfully authenticated, and who, as a result, is not able to access content on the content distribution system. For that reason, a third-party's statement or certificate vouching for the identity of an authorized user is an expression of desirability of the user as an entity that can access content from the content distribution system, *i.e.*, it is an expression of the desirability of the user as a member of the sharing group.

66. Based on the above disclosures, it is my opinion that a person of ordinary skill in the art would have reason to implement the Ganesan patent's method of authenticating the identity of a first user to a second user (by using information from a trusted intermediary) in the access control system of the Abecassis patent because use of a security certificate was a well-known way to authenticate identities on a computer network. Each method of

authentication has certain trade-offs, and security certificates signed by a trusted user tend to be more secure than a simple username and password.

67. I understand that an "invention" is obvious if it does no more than combine known elements according to a known method to yield predictable results. In my opinion, the purported invention of claims 9 and 10 of the '689 Patent does nothing more than take known elements from Abecassis (user media sharing and user access control) and combines them with known elements from Ganesan (access control based on information from a trusted user) to yield the predictable result of a media sharing group, with access to the group being determined by information from a trusted user.

68. Moreover, the combination of the Abecassis and Ganesan patents provides the teaching that applicants argued was missing from the prior art regarding the "wherein" clause present in claim 9 - "wherein the information associated with the user of the requesting media player device comprises information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group." In particular, the Ganesan patent (which was not before the Examiner during prosecution of the '689 Patent) discloses that a user may authenticate itself to another user, for purposes of receiving information from and transmitting information to the other user, by sending the other user a certificate

authenticating the first user that was produced by a trusted third party. Ganesan, 1:48 - 2:54. Thus, the concept of a trusted third party's authenticating the identity of a user so that the user can access information (*i.e.*, an indication of the desirability of the user for purposes of accessing the information) was disclosed in a prior-art reference that was not available to the Examiner during prosecution of the '689 Patent.

Docket No. 032449.0032-US04

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code.

Dated: 22-Apr-2014

Respectfully submitted,

By Kevin C Almeroth

Kevin C. Almeroth.